Technology Briefing

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

# Introduction

# Cyber terrorism is a growing concern and large-scale businesses always have a threat of cyber-attack due to ever-increasing network of cyber criminals. Several big companies have been targeted and a huge data theft has been reported in recent times. Now a days businesses comply with financial targets by using advance strategies and frameworks for money handling and for managing finances on multi national level. This include the use of financial services and international banking in order to meet the business requirements. These services are prime target of cyber criminals it is the need of time to adopt modern technological solutions in order to prevent any big financial or substantial loss. Block chain is one of the best solutions in this regard to ensure data security and managing data into blocks. This helps in managing data in chronological manner and using different mechanisms ensure data security.

# Analysis

Block Chain is used in several risk treatment strategies in order to prevent risk and possible loss to the financial transaction. In Block Chain, data blocks are followed by many other data blocks each of which carry information of financial assets and transactions in such a way that the official record of the transaction is made u of the longest chain (Cong, 2019). Block chain transactions are basis of cryptocurrency and is very useful in online financial transactions and payment.

Analyzing anomalies and their solutions in debit card transaction and security of cardholder’s personal information, PCI-DSS is very found very helpful from security point of view. PCI-DSS is the acronym of Payment Card Industry Data Security Standard and it ensure compliance in six areas. The first area of compliance is network security and the second is security and safety of user’s personal information. Third area of compliance is associated with the compatibility of vendor’s application with the industry norms and the ability interpret and reject any possible threat to the system.

For safe and secure transfer of financial assets and services, it is important with PCI (Payment Card Industry) to make sure that information of a cardholder is maintained secret and inaccessible for any person other than the owner/holder and all the other media types must also be protected. In case of remote working, if a client is working or engaged with the main network from some other place, RCR will collect his information using Microsoft Azure Key Vault to maintain control and storage (Williams, 2019).

# Summary

Companies and big firms are expanding their IT infrastructure and incorporating the use of Blockchain technologies/solutions to manage and maintain information in such a way that security is not compromised (PRITCHARD, 2019). It is very important to created didtributed ledgers to deal problems and issues in financial institutions. Not it will bring revolution in security but also will make financial transactions easy, comprehensible and with low transfer fee.

References

Underwood, S. (2016). Blockchain beyond bitcoin.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797.

Williams, B. R. (2019). *U.S. Patent No. 10,423,965*. Washington, DC: U.S. Patent and Trademark Office.

PRITCHARD, J. (2019, 12 2). *How Blockchain Is Changing Banking and Financial Services*. Retrieved from the Balance: https://www.thebalance.com/how-blockchain-is-changing-banking-and-financial-services-4174354